REMARKS

Independent claims 1, 10, 23 and dependent claim 2 have been amended as to matters of form without introducing any new subject matter. In this manner, claims 1-28 are pending in the present application. Reconsideration is respectfully requested.

In the Office Action, Applicants' specification is being objected to for informalities. By way of this amendment, page 5 of the specification is amended as to matters of form.

Claims 1-7, 10-15 stand rejected under 35 U.S.C. § 103(a) over U. S. Patent 6,260,029 ("***Critelli***") in view of U.S. Patent Application Publication 2002/0013899 ("***Faul***"). The Examiner's rejection of claims 1-7, 10-15 is respectfully traversed. Claim 1 is directed to a security envelop. The security envelop comprises a barcode in a two-dimensional symbology located on the security envelope. The barcode encodes a public component and a private component. The public component comprises a digital signature signed by the sender encrypted by the private key of the sender, and the private component comprises a digital signature signed by the sender encrypted by the public key of the receiver. Applicants respectfully submit that the rejected claim 1 is not rendered obvious in view of the applied references. To establish a *prima facie* case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim features. Additionally, the references must provide a motivation to combine in the manner suggested by the Examiner. Mere conclusory statements to combine are insufficient.

In the Office Action, the Examiner asserts that the encrypted digest 104 of the message 102 is equivalent to the public component set forth in claim 1. The encrypted digest 104 is

created and then encrypted utilizing the sender's private key. The Examiner also asserts that the public key certificate 106 element of ***Critelli*** is equivalent to the private component set forth in claim 1. The public key certificate 106 includes an identification of the certificate holder (sender) 108, the certificate holder's (sender's) public key 110 which has been digitally signed with the private key of a certificate authority (certificate authority signature 112). See ***Critelli***, col. 3, lines 15-23. Thus, ***Critelli*** teaches that the pubic key certificate 106 (which the Examiner alleges corresponds to the "private component") is signed using the private key of the certificate authority (which is neither the sender nor the receiver, but a third-party to the transaction). ***Critelli*** explains that the contents of the certificate 106 are public, and not private. ***Critelli***, col. 3, lines 34 -36 (stating that when a sender generates a SMPKC 105, the recipient verifies the authenticity of the public key certificate 106 using the certificate authority's public key.)

The Examiner appears to assert that while ***Critelli*** teaches all of the elements of claim 1, including a private component; it does not teach a private component that is encrypted by the public key of the receiver. The Applicants respectfully disagree that ***Critelli*** teaches a "private component." As noted, the Examiner argues that the public key certificate 106 is the "equivalent" to the claimed "private component" feature. However, by definition, a public key certificate is not private. Indeed, ***Critelli*** explains that any recipient having the public key of the certificate authority can verify the contents of the public key certificate. ***Critelli***, col. 3, lines 34 -36. In contrast, and as explained in the patent application, the contents of the private component are intended for the recipient who has the private key corresponding to the public key with which the contents of the private component were encrypted. Thus, contrary to the Examiner's assertion, ***Critelli*** at least fails to teach a "private component." Accordingly, for this reason, claim 1 and dependent claims are allowable. Moreover, the other pending claims are also

allowable for this reason alone.

Even assuming *arguendo* that the public key certificate 106 corresponds to the "private component" as alleged in the Office Action, the Examiner's obviousness rejection still falls short, as explained below. Claim 1 calls for encrypting the private component using the public key of the receiver. The Examiner argues that ***Faul*** teaches encrypting the private component using the public key of the receiver because ***Faul*** teaches encrypting "non-essential" elements (which, according to the Examiner, correspond to the "private component" of ***Critelli***) using the receiver's public key. The Examiner's reliance on the combination of ***Critelli*** and ***Faul*** is misplaced.

To establish a prima facie case of obviousness, there must be a teaching in the references that suggest the combination advanced by the Examiner. Here, the Examiner provides no motivation other than a mere conclusory statement that it would be obvious to combine the references in the manners suggested. Such a conclusory statement is inadequate to establish a prima face case of obviousness. Notwithstanding the Examiner's failure to provide any substantive motivation to combine, a closer review of ***Critelli*** and ***Faul*** reveals that not only do these references fail to provide any requisite motivation to combine, they, in fact, teach away from the claimed combination.

The Examiner first relies on ***Critelli*** to show a "private component." As noted, according to the Examiner, the public key certificate 106 corresponds to the "private component" of claim 1. Further, the Examiner asserts that the "non-essential" elements of ***Faul*** correspond to the "public key certificate 106" of ***Critelli***, and that these non-essential elements are encrypted using

the public key of the receiver. While the Examiner alleges that the non-essential elements, (*i.e.*, the private component of ***Critelli,*** according to the Examiner) are encrypted using the receiver's public key, the Examiner overlooks that ***Critelli*** teaches that the "public key certificate 106" is signed by the private key of a certificate authority, which means that anyone having access to the counterpart public key can access the contents of the public key certificate 106. *See* col. 3, lines 34 -36. The Examiner's suggestion of combining the "non-essential" elements of ***Faul*** with the teachings of ***Critelli*** thus fails because ***Critelli*** teaches away from the notion of using a public key of the receiver (as claimed). Indeed, using a pubic key of the receiver for the purposes of the "public key certificate 106" would render such a certificate not public (because, under such a scenario, only the recipient with the private key could decrypt the contents). Stated differently, the Examiner's proposed combination of applying the teachings of ***Faul*** (which according to the Examiner teaches encrypting using a public key of a receiver) runs contrary to the teachings of ***Critelli*** (which states that the certificate 106 is intended to be public, namely a "public key certificate 106"). Accordingly, for this additional reason, the pending claims are allowable.

The Examiner also relies on U.S. Patent No. 5,917,925 (***Moore)*** to reject some of the dependent claims. However, ***Moore*** fails to address the above-addressed shortcomings of ***Critelli*** and ***Faul***.

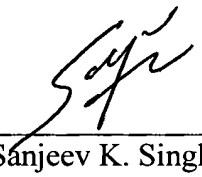
Arguments with respect to other dependent claims have been noted. However, in view of the aforementioned arguments, these arguments are moot and therefore not specifically addressed. To the extent that characterizations of the prior art references or Applicants' claimed subject matter are not specifically addressed, it is to be understood that Applicants do not

acquiesce to such characterization. Reconsideration of the present application is respectfully requested.

In light of the arguments presented above, Applicants respectfully assert that all of the claims are allowable. Accordingly, a Notice of Allowance is respectfully solicited.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned patent agent at the Houston, Texas telephone number (713) 934-4089 to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,



Date: September 1, 2005
CUSTOMER NO. 23720

Sanjeev K. Singh, Ph.D
Rec. No. L0220
WILLIAMS, MORGAN & AMERSON
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-4089
(713) 934-7011 (facsimile)
AGENT FOR APPLICANTS